UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
----------X
UNITED STATES OF AMERICA,

17 CR 569 (ER)

-against-

JAMES BECKISH, *et al.*,

Defendants.
----------X

MEMORANDUM SUPPORTING JOINT PRETRIAL MOTIONS FOR DEFENDANTS JAMES BECKISH AND JOSEPH ANTHONY DEMARIA

LAW OFFICE OF MARC FERNICH
810 Seventh Avenue
Suite 620
New York, NY 10019
Ph: (212) 446-2346

Attorneys for James Beckish

LAW OFFICES OF JEFFREY LICHTMAN
11 East 44th Street
Suite 501
New York, NY 10017
Ph: (212) 581-1001

Attorneys for Joseph Anthony DeMaria

TABLE OF CONTENTS

STATEMENT

James Beckish and Joseph Anthony DeMaria seek multiple relief against an indictment charging them and three codefendants – James Toner, Richard Witcher and Peter O'Brien – with one count each of wire fraud (18 U.S.C. § 1343), wire fraud conspiracy (*id.* § 1349) and aggravated identity theft (*id.* § 1028A).

ARGUMENT

POINT I

COUNTS ONE AND TWO – LACKING ESSENTIAL OFFENSE ELEMENTS – ARE IMPERMISSIBLY VAGUE AND FAIL TO CHARGE COGNIZABLE CRIMES, DEMANDING THE INDICTMENT'S DISMISSAL

Counts One and Two of the indictment purport to allege substantive and conspiratorial wire fraud offenses – prototypical "darling[s]" of the "prosecutor's nursery." *Harrison v. U.S.*, 7 F.2d 259, 263 (CA2 1925) (L. Hand, J.). Parroting 18 U.S.C. § 1343's famously supple text, the counts accuse the defendants – in their lone case-specific clauses – of "creat[ing] and operat[ing] websites that they used to place millions of dollars of unauthorized and recurring charges on credit card accounts belonging to at least tens of thousands of victims." Ind. ¶¶ 1-3. That's the sum of the charged factual claims – save that the conduct assertedly occurred over a four-year period, from 2013 to 2017, in this District and "elsewhere." *Id.* ¶¶ 1, 3.

Granted, an indictment need only contain a "plain, concise, and definite … statement of the essential facts constituting the offense"[1] to "fulfill" its main offices – namely, "notifying" the accused of the "charges" so he can prepare a defense and assuring he's "tried [solely] on the matters considered by the grand jury." *U.S. Pirro*, 212 F.3d 86, 93 (CA2 2000); *see*, *e.g.*, *U.S. v. Walsh*, 194 F.3d 37, 44-45 (CA2 1999) (to satisfy Fifth and Sixth amendments, indictment must also include "enough detail" to protect against double jeopardy "in a future prosecution based on the same set of events") (citation, internal quotation marks and footnote omitted). And, admittedly, it usually "suffic[es]" to "track[] the language of the statute charged and state[] the time and place (in approximate terms) of the alleged crime." *Pirro*, 212 F.3d at 92-93 (internal citation and quotation omitted).

Not so, however, for "generic[ally]" defined offenses[2] involving falsity and fraud. *See U.S. v. Stringer*, 730 F.3d 120, 127 (CA2 2013) (collecting cases). When "a charge is brought under [a] generally-worded provision"[3] like § 1343, "an indictment must do more than simply repeat"[4] sweeping "statutory language." *U.S. v. Curtis*, 506 F.2d 985, 990 (CA10 1974). Instead it "must descend to particulars,"[5] specifying the "theory on

[1] Fed. R. Crim. P. 7(c)(1).

[2] *Pirro*, 212 F.3d at 92-93 (citations and internal quotes omitted).

[3] *U.S. v. Smolar*, 557 F.2d 13, 19 (CA1 1977).

[4] *Stringer*, 730 F.3d at 126 (citation and quotation marks omitted).

[5] *Pirro*, 212 F.3d at 93 (citations and internal quotes omitted).

which it [alleges] acts [] and practices … which operated and would operate as a fraud and a deceit." *Smolar*, 557 F.2d at 19 (citation and internal quotes omitted).

Put differently, a "criminal defendant" is constitutionally "entitled to an indictment that states the essential elements" of the "charged" offense. *Pirro*, 212 F.3d at 91-92. And when a given element is "implicit" rather than "explicit" in a broadly framed "statute,"[6] the indictment must "spell[] out" how the "particular element" will be "met" – not merely offer a "categorical recitation of the element." *Stringer*, 730 F.3d at 126. Conversely, an indictment that simply "tracks the language of the statute and fails to allege the implicit element explicitly" flouts the "Fifth and Sixth [a]mendments" and fails to "allege an offense," compelling dismissal. *Pirro*, 212 F.3d at 92-93 (internal citations and quotation omitted); *see*, *e.g.*, *U.S. v. Smith*, 985 F. Supp. 2d 547, 561 (SDNY 2014), *aff'd*, *U.S. v. Halloran*, 664 F. App'x 23 (CA2 2016), *cert. denied*, *Smith v. U.S.*, 138 S. Ct. 56 (2017).

Among the essential elements of a wire fraud violation – whether implicit or explicit – is the presence of a "material misrepresentation." *Williams v. Affinion Grp., LLC*, 899 F.3d 116, 124 (CA2 2018) ("material misrepresentation" necessary to establish scheme to defraud) (citing *Neder v. U.S.*, 527 U.S. 1, 25 (1999)).[7] Yet the fraud

---

[6] *Ibid.*

[7] *Accord*, *e.g.*, *U.S. v. Binday*, 804 F.3d 558, 576-77 (CA2 2015) (defendants must make "misrepresentations" that "deprive[]" victims of "economically valuable information that bears on their decision-making"); *McEvoy Travel Bureau Inc. v. Heritage Travel, Inc.*, 904 F.2d 786, 791 (CA1 1990) ("scheme must be intended to deceive" by "false or fraudulent pretenses, representations, promises, or other deceptive conduct") (emphasis deleted); *cf. Cleveland v. U.S.*, 531 U.S. 12, 25-26 (2000)

charges here give no substantive inkling of any misrepresentations *at all* – let alone material ones affecting an "essential element of the bargain," implicating the "nature and quality" of the goods and services provided, or otherwise having "relevan[ce] to the object of the contract." *Binday*, 804 F.3d at 570-71 & nn. 10-11 (citations and quotation marks omitted); *cf. U.S. v. Klein*, 476 F.3d 111, 113-14 (CA2 2007) (inferring "an allegation of materiality," on plain error review of bank fraud indictment, from recitation of statutory language coupled with properly pleaded claims of "misleading conduct [and] speech").

Instead, as noted, counts One and Two merely juxtapose a bare invocation of the pertinent statutory phrase – "false and fraudulent pretenses, representations, and promises" – with an inscrutable assertion of "unauthorized and recurring [credit] charges" placed through websites. Ind. ¶¶ 1-3. That sort of cryptic charging technique encourages amendment, variance and unfair surprise, inviting the government to shift theories as convenient by "fill[ing] in elements of its case with facts other than those considered by the grand jury." *Pirro*, 212 F.3d at 92 (citation and internal quotations omitted). And it's the very evil that the Fifth and Sixth amendments plus Criminal Rule 7 – as elaborated in the generic offense cases surveyed earlier – strive to prohibit.

(coextensive mail fraud statute proscribes a single crime rather than separately punishing schemes to defraud and schemes to obtain money or property by means of false or fraudulent pretenses, representations or promises).

Indictments are routinely condemned or discarded, in this Circuit and elsewhere, for similar facial flaws.[8]

Indeed, our own court of appeals threw out a wire fraud charge that *did* allege concrete misrepresentations – the defendant falsely promised to export a chemical he bought from a counterparty – but espoused an invalid materiality theory sounding in fraudulent inducement or transaction causation – *i.e.*, the counterparty "would not have sold" the chemical "had it known" the defendant "in fact intended to [re]sell the product domestically." *U.S. v. Shellef*, 507 F.3d 82, 109 (CA2 2007) ("legally [in]sufficient" indictment "states only" that defendant's "misrepresentation" induced counterparty to enter a transaction it "would otherwise have avoided").

How much worse a fraud indictment missing both false representations *and* any indication of their putative materiality – thus making the charged materiality theory impossible to ascertain or evaluate for legal sufficiency? The question answers itself and calls for the same result. *Cf.*, *e.g.*, *Williams*, 899 F.3d at 124 n.5 (plaintiffs cannot "avoid pleading a material misrepresentation in the scheme to defraud"); *U.S. v. Davis*, No. 13-

[8] *E.g.*, *U.S. v. Yefsky*, 994 F.2d 885, 888-89, 893 (CA1 1993) (stock statutory assertion that codefendant obtained money through false pretenses, without divulging factual basis or specifying pretenses used, failed to "describe fraudulent conduct," sufficiently identify fraudulent plan or provide "adequate notice"); *U.S. v. Tonelli*, 577 F.2d 194, 200 (CA3 1978) (vacating conviction where indictment "did not set forth the precise falsehoods alleged and the factual bases of their falsity with sufficient clarity to permit a jury to determine their verity and to allow meaningful judicial review of the[ir] materiality") (cited approvingly in *Stringer*, 730 F.3d at 126-27); *U.S. v. Nance*, 533 F.2d 699, 701 (CADC 1976) (dismissing indictment lacking "any allegation whatsoever" as to what "false pretenses were"); *Curtis*, 506 F.2d at 890 (statutory language insufficient without "substantial indication" of "false pretenses, representations, or promises"); *U.S. v. Josten*, 704 F. Supp. 841 (N.D. Ill. 1989) (tossing mail fraud indictment for failure to specify means, methods and misrepresentations).

cr-923 (LAP), 2017 WL 3328240, at *26-*28 (SDNY Aug. 3, 2017) (sustaining indictment, under "liberal interpretation" governing belated "sufficiency" challenge first raised near trial's end, that detailed fraudulent minority- and woman-owned business claims defendants filed and explained why they were fraudulent).

As *Shellef* suggests, an indictment's wholesale omission of identifiable misrepresentations is no mere technical defect. After all, not "every transaction induced by deceit" is "actionable under the mail and wire fraud statutes." *Binday*, 804 F.3d at 570. Rather, as the Second Circuit recently reiterated, the deceit must deprive the victim

> "of potentially valuable economic information." *U.S. v. Wallach*, 935 F.2d 445, 463 (CA2 1991). "Our cases have drawn a fine line between schemes that do no more than cause their victims to enter into transactions they would otherwise avoid – which do not violate the mail or wire fraud statutes – and schemes that depend for their completion on a misrepresentation of an essential element of the bargain – which do violate the mail and wire fraud statutes." *Shellef*, 507 F.3d at 108.

Binday, 804 F.3d at 570. Absent enumeration, there's no way to know whether the "false and fraudulent pretenses, representations, and promises"[9] put before the grand jury in our case fall on the right or wrong – the actionable or inactionable – side of the "line." *Shellef*, 507 F.3d at 108.

This concern is especially acute in the circumstances at hand. The crux of the complaint that led to defendants' arrest is that they "obtained" stolen "credit card

[9] Ind. ¶¶ 1-3.

numbers in bulk by buying them on the black market," using the numbers to make "unauthorized and recurring charges" through a network of websites they operated. Complaint ¶ 6; *see also*, *e.g.*, *id.* ¶ 10 ("defendants' fraudulent scheme depended on replenishing the supply of stolen credit cards that could be used to make new, and recurring, fraudulent charges"); *id.* ¶ 11 (defendants "operat[ed] multiple websites in order to make fraudulent charges on stolen credit cards").

For their part, defendants contend – and the evidence will show – that they (A) lawfully purchased the accounts of customers who'd signed up to receive recurring shipments of nutraceutical products[10] from other online vendors, and (B) continued to service the accounts by sending the customers generic equivalents. If defendants are correct, the indictment fails to charge a crime; the customers got substantially what they bargained and paid for. More precisely, "there was no discrepancy between benefits reasonably anticipated and actual benefits received,"[11] rendering any false "pretenses, representations, and promises" aimed at the customers immaterial as a matter of law. Ind. ¶¶ 1-3. And even if defendants are wrong, stealing credit cards and using them to make unauthorized charges is more consistent with theft or larceny than fraud – at least vis-à-vis the cardholders, and at least in the absence of articulated misrepresentations.

[10] According to the complaint, "'nutraceuticals'" include "dietary supplements and similar products." Complaint ¶ 6.

[11] *U.S. v. Starr*, 816 F.2d 94, 98-99 (CA2 1987) (internal quotation marks and citation omitted).

There are other problems as well. Like the indictment, the complaint and search warrant affidavits in the case are bereft of specific falsehoods allegedly attributable to defendants. But a review of those documents suggests a menu of potential deception targets: (A) the individuals whose credit cards were supposedly stolen or acquired on the black market; (B) visitors to the websites defendants operated; (C) consumers contacting call centers they ran; and/or (D) a spate of credit card processing companies, including but not limited to First Data and First Pay Solutions. Adding to the ambiguity, the complaint and warrant affidavits imply that the processors – if among the ostensible targets – could have been misled in a variety of plausible ways: in either (1) defendants' applying for merchant identification numbers; (2) their submitting transactions for processing; (3) their responding to fraud prevention inquiries; or (4) some combination of the three. Against that amorphous backdrop, counts One and Two not only fail to allege cognizable crimes, but also flunk the indictment's core notice function, leaving defendants to guess at the thrust of the charge they must meet.

In sum, material misrepresentations are indispensable ingredients of wire fraud. Because they fail to adequately allege *any* misrepresentations – much less material ones – counts One and Two are deficient on their face. And since Count Three – charging aggravated identity theft under 18 U.S.C. § 1028A – hinges on the validity of counts One and Two, it too must fall, mandating outright dismissal.

POINT II

DEFENDANTS ARE ENTITLED TO A LIMITED BILL OF PARTICULARS

As discussed in **POINT I**, the indictment's wire fraud counts, in their entirety, pair a bald recital of 18 U.S.C. § 1343's elastic text with the impenetrable claim that defendants made "unauthorized and recurring" credit card charges via "websites" they "created and operated." Ind. ¶¶ 1-3. For the reasons **POINT I** explains, those counts not only fail to plead cognizable crimes, but provide insufficient notice of the accusations defendants must contest. Though it can't cure a defective indictment,[12] a limited bill of particulars is thus minimally warranted barring straight up dismissal.[13]

Specifically, the bill should identify (A) the allegedly false representations ascribed to defendants[14]; (B) the theory or theories of fraud the government asserts,[15]

---

[12] *Walsh*, 194 F.3d at 45.

[13] As Ex. A reflects, the parties conferred in good faith regarding defendants' request for particulars but couldn't reach agreement. *See* Local Crim. R. 16.1.

[14] *E.g.*, *U.S. v. Bortnovsky*, 820 F.2d 572, 574-75 (CA2 1987) (reversing conviction for denial of bill of particulars identifying fraudulent documents); *U.S. v. Vaid*, No. 16-cr-763 (LGS), 2017 WL 3891695, at *11 (SDNY Sept. 5, 2017) (ordering bill identifying fraudulent claims – and collecting authorities ordering bills specifying fraudulent "documents" and "transactions" in "cases involving fraud").

[15] For instance, the complaint – but not the indictment's four corners – claims defendants "obtained credit card numbers in bulk by buying them on the black market and by capturing the credit card numbers of individuals who sought to make legitimate purchases through the Websites." Complaint ¶ 6; *cf. Stringer*, 730 F.3d at 124-25 (discovery – like bill of particulars – can't save defective indictment) (citing *Walsh*, 194 F.3d at 45). But nothing in the indictment, discovery or any other source explains how either allegation amounts to stealing credit cards – let alone defrauding cardholders. *See* Complaint, *e.g.*, ¶¶ 10-11. After all, the mere contention that some customers got no product (*id.* ¶ 6) doesn't rise to fraud unless defendants never intended to send them any – a suggestion found nowhere in the indictment or any place else. *E.g.*, *Puckett v. U.S.*, 556 U.S. 129, 138 n.1 (2009) ("It is hornbook law that misrepresentation requires an intent *at the time of contracting* not to perform.") (citation omitted).

in part to permit an informed legal determination whether the alleged misrepresentations rank as economically material[16]; and (C) the categories of alleged victims the government posits – *e.g.*, credit card holders, credit card processors or both – naming any processors included.[17] These bare essentials are necessary to enable defense preparation, prevent surprise and protect against future jeopardy for the same conduct. *Bortnovsky*, 820 F.2d at 574 (listing purposes of bill of particulars).

POINT III

FRUITS OF THE NOV. 2015 GOOGLE WARRANT MUST BE SUPPRESSED

On Nov. 16, 2015, the government obtained a search warrant ordering Google to produce records from three email accounts subscribed to codefendants Beckish and Witcher. Warrant and Affidavit (Ex. B). The government suspected certain "Subject Companies" – never identified – of fraudulently placing "unauthorized and recurring charges on victims' credit cards." Warrant Aff. ¶ 8. Beckish moves to suppress all fruits

[16] *E.g.*, Vaid, 2017 WL 3891695, at *11 (directing bill explaining how and why each allegedly fraudulent insurance claim was fraudulent – *viz.*, "whether the goods or service was not provided or was medically unnecessary"); *U.S. v. Nachamie*, 91 F. Supp. 2d 565, 574-75 (SDNY 2000) (directing bill specifying manner in which each entry, statement or item on every document claimed to be fraudulent was false or misleading); *cf. U.S. v. Barnes*, 158 F.3d 662, (CA2 1998) (bill of particulars required as necessary to prepare defense even if it discloses prosecution "theories").

[17] *E.g.*, *Stringer*, 730 F.3d at 127 (victim identity "is of course an essential element of the charge, unquestionably important, and the defendant is of course entitled on demand to its disclosure in a bill of particulars or otherwise").

– direct and derivative – of his ensuing account search, arguing that the affiant materially misled the issuing judge.[18]

A. THE PROFFERED CAUSE WAS MISLEADING AND INACCURATE

Probable cause rested principally on a few scant assertions:

- A "heightened charge-back ratio suggests that the Subject Companies are engaged in fraudulent activity." *Id.* ¶ 9c.

- "[A]n online message board [] includes complaints regarding certain products sold by certain of the Subject Companies." *Id.* ¶ 10. The anonymous internet posts were lengthy and detailed but unverified:

    - In a Sept. 16, 2014 post, a purported former call center employee claimed that "[e]verything is 100% scam, of course nobody ordered this product and of course It was never sent." *Id.*

    - In a Sept. 17, 2014 post, a purported customer asserted the "[p]erpetrators" were "using stolen … names, addresses, and [credit card or bank information] to post an unauthorized charge of $49.95." *Id.* ¶ 11.

    - In a Sept. 24 reply, a purported "ex-employee" claimed that "lists of customers" were bought so they could be charged for "a dietary supplement," in addition to "real accounts" that actually "purchase[d] the supplement." *Id.*

- "[R]ecords maintained by the Better Business Bureau" indicate that "approximately 300 complaints" – ostensibly matching the affiant's proffered fraud "narratives" – have been "filed against certain Subject Companies." *Id.* ¶ 12.

[18] Though the affidavit was sworn by Secret Service agent Erin Thackston, the warrant ascribed it to "Special Agent John Wozniak" (Warrant ¶ 1), suggesting "the magistrate" may have acted more as a "rubber stamp" and less a "neutral and detached" intermediary between state and targets. *U.S. v. Leon*, 468 U.S. 897, 914 (1984). That's especially so where the affidavit purported to establish "probable cause" as to "stalking," a phantom federal crime. Warrant Aff. ¶ 3.

But a string of "reckless" falsehoods tainted the proffered cause, requiring "exclusion of the seized evidence." *U.S. v. Franks*, 438 U.S. 154, 167, 171 (1978). First, the affiant asserted that "[f]or most businesses, a charge-back rate of approximately 1% is normal." Warrant Aff. ¶ 9b. That oversimplification left out important qualifiers. A "chargeback" is a "transaction that an issuer returns to an acquirer." Card Acceptance Guidelines for Visa Merchants, at 68.[19] In other words, it occurs when a consumer's credit card company dishonors a charge. For some industries the rate is low – but not the industry in question. "Chargeback rates vary substantially, depending on type of industry and merchant revenue." The State of Chargebacks: 2018 Report, at 4.[20] And when it comes to online transactions, chargeback rates routinely eclipse those for brick and mortar industries.

For example, "[n]early 30 percent of organizations selling any type of digital goods or services report chargeback rates of 1 percent or higher, compared to 21 percent of merchants selling only tangible or shippable goods." *Id.* "In fact, merchants selling digital goods and services appear to be more comfortable managing a higher optimum chargeback rate." *Id.* "Based on [] analysis of three billion transactions across 18 industries," one company compiled a "table of chargeback ratios (total chargebacks

[19] https://usa.visa.com/dam/VCOM/download/merchants/card-acceptance-guidelines-for-merchants.pdf (last visited 7/11/18).

[20] https://www.jhacanada.com/content/images/White_Paper-The_State_of_Chargebacks_2018.pdf (last visited 7/11/18).

divided by total transactions)" showing "internet" commerce to have the highest.[21] As one might expect, "explosive year-over-year growth in eCommerce" means that "[m]erchants are finding themselves in more situations where the card and cardholder are not present," boosting chargeback rates. Card Acceptance Guidelines for Visa Merchants, at 41.[22] But the affiant deprived the issuing judge of that broader context.

The affiant next averred that "[t]he average charge-back rate for the Subject Companies for the 12-month period ending … February 2015 was approximately 23%." Warrant Aff. ¶ 9c. That figure also eschewed key details. On Sept. 9, 2014, First Pay Solutions – the company that processed the credit card payments – "disabled" the merchant accounts for several Subject Companies, meaning "refunds" couldn't be processed and causing chargebacks to artificially spike. 9/4/14 email (Ex. C) at 33; 9/30/14 email ("chargebacks are huge this month because we cannot refund … [and it's] not our fault our customers need to Chargeback when they legitimately are owed a refund") (Ex. D).[23] As a result, an agreement attributing the chargeback "problem" to the "suspension of Refunds post-termination" was duly negotiated. 10/28/14 transmittal email and unsigned MOU[24] (Ex. E) at 6 (original to follow as available).

---

[21] http://www.optimizedpmts.com/understanding-and-reducing-chargebacks/ (last visited 6/21/18).

[22] https://usa.visa.com/dam/VCOM/download/merchants/card-acceptance-guidelines-for-merchants.pdf (last visited 7/11/18).

[23] All nonpublic exhibits come from the government's discovery production.

[24] The MOU identifies Jay Wigdore, who should have been viewed skeptically, as controlling First Pay. In 2017 the FTC sued Wigdore for his 2012 participation in a "deceptive telemarketing scam" in which

"This issue [was] not the fault of the [Subject Companies] but rather the fault of First Data [] and First Pay." *Id.* Again withholding fuller context, the affiant spun "this heightened charge-back ratio" as evidence of "fraudulent activity." Warrant Aff. ¶ 9c.

The government must have known the exculpatory information because in seeking the warrant, the affiant relied on "another USSS agent ("Agent-1"), who has corresponded with representatives of First Data and First Pay Solutions, which are associated online payment processors … [used by] the Subject Companies." *Id.* ¶¶ 9, 9a, 14 ("Agent-1 … has corresponded with representatives of First Pay [] and received records of communications from certain individuals associated with the Subject Companies to First Pay Solutions").

It is not plausible that the Secret Service questioned First Pay about the Subject Companies in 2014-15 without discussing the Sept. shutdown. *See, U.S. v. Rajaratnam*, 719 F.3d 139, 154 (CA2 2013) ("factfinder may infer reckless disregard from circumstances evincing obvious reasons to doubt the veracity of the allegations"); *U.S. v. Reilly*, 76 F.3d 1271, 1280 (CA2 1996) (inferring "recklessness" where "officers [] fail to provide all potentially adverse information to the issuing judge").

Indeed, the affidavit highlighted an Oct. 24, 2014 Beckish email on that very topic in claiming he used the gmail account to discuss the Subject Companies. Warrant

---

the independent sales organization he ran played a similar role to First Pay's here. Related FTC defendants had "settled in 2015" whereas the Google warrant issued in Nov. of that year. *FTC v. Electronic Payment Services, et al.*, No. 17 CV 2535 (D. Ariz.), ECF No. 1 ¶¶ 4, 57.

Aff. ¶ 14(a)-(b). With the operative emails only a few days apart and addressed to the same recipients at First Pay, it is difficult to accept that the affiant didn't know how the same issue arose or was resolved.

B. AN ACCURATE DESCRIPTION OF THE BUSINESS ACTIVITY WOULD NOT HAVE ESTABLISHED PROBABLE CAUSE

"To suppress evidence obtained pursuant to an affidavit containing erroneous information, the defendant must show that: (1) the claimed inaccuracies or omissions are the result of the affiant's deliberate falsehood or reckless disregard for the truth; and (2) the alleged falsehoods or omissions were necessary to the issuing judge's probable cause [] finding." *Rajaratnam*, 719 F.3d at 146. "To determine if misrepresentations or omissions are material, a court corrects the errors and then resolves de novo whether the hypothetical corrected affidavit still establishes probable cause." *U.S. v. Lahey*, 967 F. Supp. 2d 698, 711 (SDNY 2013) (agents misrepresented sequence of events during motorcycle club party and omitted other information to convey false impression that individuals set up guard duty expressly to protect drug deals). "Where a defendant makes [such] a preliminary showing," *Franks* "instructs a district court to hold a hearing to determine whether the alleged misstatements … were [] intentional [or] reckless [and] material." *Rajaratnam*, 719 F.3d at 146.

The Court must "evaluate the tendency and force of [the misstated evidence] item by item; there is no other way." *Cf. Kyles v. Whitley*, 514 U.S. 419, 436 n.10 (1995) (addressing materiality of suppressed *Brady* evidence). The Court then "evaluate[s] its

cumulative effect for purposes of materiality separately and at the end of the discussion." *Id.*

Here, it is "obviously problematic" that the misstatements all "drive in the same direction" – exalting the chargebacks' extent and import while concealing a major external cause – to "establish[]" an inference of fraud that "the fuller evidence did not support." *Lahey*, 967 F. Supp. 2d at 723. Indeed, a fairer presentation would have left "a thin reed on which to base a" full blown search of Beckish's entire email account. *Cf. id.* at 724-25 (defendant's "membership in the Pagans [motorcycle gang] does not, by itself, establish probable cause to search his residence").

In short, the government conjured probable cause by coupling inflated chargeback rates with a vague summary of Better Business Bureau complaints and anonymous internet postings. In the government's telling, Bureau records indicated that "approximately 300 complaints have been filed against certain Subject Companies." Warrant Aff. ¶ 12. Forgoing any detail,[25] the affiant proffered that *another* agent's "review of the narratives associated with these complaints … align[s] with [a] scheme [whereby] consumers' credit cards were charged for nutraceutical products that were never ordered and/or never provided." *Id.*

In fact, the absolute number of complaints – whether 100 or 300 – proved little without the relative context of overall business volume. To that end, discovery reveals

[25] On information and belief, it appears that the Bureau's subpoena return included a batch of companies unaffiliated with Beckish. Excluding them cuts the number of complaints to 137.

more than 140,000 shipping confirmations between Nov. 2013 and April 2015. And that only includes invoices or shipping confirmations attached to seized emails. It's not even a complete list of units shipped. Against six figures worth of shipped units, a few hundred customers making unverified complaints is wholly unremarkable and certainly doesn't equate to criminality. *Cf. Williams*, 889 F.3d at 120-22 ("plaintiffs' failures of recollection or bare denials" that they enrolled in online membership discount programs doesn't mean it didn't happen).

As for the internet postings, "anonymous informant" tips also fall short of "probable cause" if "[in]sufficiently corroborated." *U.S. v. Elmore*, 482 F.3d 172, 179 (CA2 2007). On "a sliding scale," the degree of anonymity determines the necessary level of corroboration. *Id.* at 181. "Where the informant is completely anonymous" the maximum "amount of corroboration will be required" (*id.*) as "the veracity of persons supplying anonymous tips is … unknowable." *Ala. v. White*, 496 U.S. 325, 329 (1990) (partially corroborated tip from completely anonymous informant presented a "close case" establishing only reasonable suspicion, largely because it "predict[ed] future behavior"); *Florida v. J.L.*, 529 U.S. 266 (2000) (observing that "anonymous tips … are generally less reliable" and holding insufficient to establish even reasonable suspicion a completely anonymous tip that a young black man in a plaid shirt at a designated bus stop had a gun).

To be sure, the *White* and *J.L.* tipsters had actual verbal communication with police in real life. Here, by contrast, the digital nature of the anonymous complaints

further relieved the authors of any "risk that [they] will be held accountable if [their] information proves false." *Elmore,* 482 F.3d at 181. "[A]nonymous comments sections" are notoriously unreliable, one Pulitzer Prize winner branding them "havens [of] factual inaccuracy."[26] Unlike a real-world tipster who physically talks to a cop, internet posters are unlikely to think that law enforcement will act upon their information – or to believe that falsehoods might have consequences.

For example, even anonymous "911 call[s]" have "some features that allow for identifying and tracing callers, and thus provide some safeguards against making false reports with immunity." *Navarette v. Calif.*, 134 S. Ct. 1683, 1689 (2014) ("opportunity to identify" a "false tipster's voice" helped establish only "reasonable suspicion" in another "close case"). Yet even that minimal safeguard, or something analogous, is absent as to anonymous internet posters on third party websites. Perhaps the anonymous posts could've established bases of knowledge. But no indicia of veracity can be found. Nothing about the posts was corroborated – whether poster identity, historical or predictive information.

The anonymous tips had other problems too. Lack of corroboration aside, the disgruntled employees were openly biased and their complaints internally inconsistent. Warrant Aff. ¶ 10 ("I have my reasons to report this company"). On the one hand, a

[26] https://www.washingtonpost.com/news/monkey-cage/wp/2014/08/19/its-time-to-end-anonymous-comments-sections/?noredirect=on&utm_term=.39ff9c07ef18 (last visited 6/21/18).

purported customer "service" employee claimed to be "just [an] agent[] answering the phone" and "doing [her] job" – a corporate cog operating on limited knowledge. *Id.* But on the other hand, the same self-styled functionary somehow professed to know that "[e]verything is 100% scam, of course nobody ordered this product and of course it was never sent." *Id.* Which one was it?

In any case, the government's own discovery shows over 100,000 units shipped, belying any suggestion that the business was "100% scam." Compare *id.* with *id.* ¶ 11 ("there are actual real accounts"). Even better, the various posters flatly contradicted each other in central respects. Compare *id.* ¶ 10 ("we had to lie as much as possible to save the refunds") with *id.* ¶ 11 ("[a]nother important detail is that ALWAYS, if a customer requests for refund on a fake account, you give back the money").

Still other accusations betray an elusive if not illusory basis of knowledge. *Id.* ¶ 11 ("bosses buys this lists of customers in black market *if im not wrong*") (emphasis supplied)). Some also contain multiple levels of hearsay, one anonymous tipster recounting what another supposedly said. *Id.*

Vagueness reigned as well. For one, the supposed 300+ Better Business Bureau complaints were never described in any detail. Instead, they were merely alleged to concern "certain Subject Companies." *Id.* ¶ 12. Well, which companies? How did the government purport to tie them to defendants? What did the complainants actually say? The affiant didn't explain so the issuing judge couldn't decide. *Id.*

Far from meshing, the anonymous web posts didn't come close to forming a coherent fraud narrative. The affiant averred "that the Target Subjects are engaged in a fraud whereby the Subject Companies are used to place unauthorized and recurring charges on victims' credit cards." *Id.* ¶ 8. "Credit card numbers are either obtained through surreptitious means, or by virtue of individuals making purchases through the Target Companies' websites." *Id.* Shorn of the incomplete and misleading chargeback statistics, that sort of enigmatic fraud theory doesn't begin to approach probable cause. What "surreptitious means" were used? How did the government – or defendants – know the card numbers were stolen? What does "unauthorized and recurring" actually mean?

Correcting the affiant's mischaracterizations, insufficient cause supported the warrant.

C. THE GOVERNMENT IMPROPERLY REVIEWED AND DISSEMINATED TENS OF THOUSANDS OF PRIVILEGED EMAILS

Beyond the *Franks* violation, attorney-client privilege infractions cumulatively counsel suppression.[27] Specifically, the government obtained, presumably reviewed and disseminated tens of thousands of "protect[ed] communications (1) between a client and his or her attorney (2) that are intended to be, and in fact were, kept confidential

[27] This branch of the motion applies to both defendants. A DeMaria gmail account was among the targets of a subsequent warrant.

(3) for the purpose of obtaining or providing legal advice." *U.S. v. Meija*, 655 F.3d 126, 132 (CA2 2011). The privilege is among the "oldest" and most venerable because "full and frank communication between attorneys and their clients [] promote[s] broader public interests." *Upjohn Co. v. U.S.*, 449 U.S. 383, 389 (1981).

It's a given that "prosecution team" members must not "view[] any privileged materials or learn[] any privileged information … uncovered" during a search. *U.S. v. Stewart*, 02 CR 396 (JGK), 2002 WL 1300059, at *3 (SDNY 2002) (appointing special master to review seized legal files); *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, U.S. Dept. of Justice, Jan. 14, 2005,[28] at 110 ("a trustworthy third party must examine [a seized] computer to [shield] the prosecution team [from] privileged material").

"Agents must exercise special care when planning a computer search that may result in the seizure of … attorney-client communications." *Id.* at 109. Accordingly, they should "devise a strategy for reviewing the seized computer files following the search so that no breach of a privilege occurs." *Id.*

But the digital search protocols here ignored privilege entirely. Instead, they focused exclusively on identifying relevant documents:[29]

---

[28] https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf (last visited 6/12/18).

[29] Digital "searches … raise unique Fourth Amendment issues," such as the worrisome "intermingling of relevant documents with documents that the government has no probable cause to seize." *U.S. v. Vilar*, No. 05 CR 621, 2007 WL 1075041, at *35 (SDNY 2007). Even if the warrant is upheld, the Court must order expungement of records outside the warrant's scope, lest law enforcement "simply

> law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all emails within the Subject Account. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.

E.g., Warrant Aff. ¶ 21; compare *Searching and Seizing Computers,* at 110 (affidavit should describe "post-seizure strategy for screening out … privileged files").

Here, Google disclosed tens of thousands of privileged emails to the government. For Beckish, out of 180,678 total emails, some 21,921 were privileged – roughly 12 percent.[30] For DeMaria, out of 62,525 total emails, some 6125 were privileged – roughly nine percent. "One would expect that [the government's] reasonable review of the evidence would detect some privileged documents if there are

keep all of the data it collects, regardless of its relevance to the specific investigation for which it is sought and whether the warrant authorized its seizure." *In the Matter of a Warrant for all Content and Other Information Associated with the Email Account xxxxx@gmail.com Maintained at the Premises Controlled by Google, Inc.*, 33 F. Supp. 3d 386, 396 (SDNY 2014); *U.S. v. Ganias*, 824 F. 3d 199, 218 (CA2 2016) ("recourse" for "parties with an interest in retained storage media" includes "motion to the court" to parse "the reasonableness of seizure and subsequent retention by the government of such vast quantities of irrelevant private material").

[30] Ex. F and G contain privilege logs for Beckish and DeMaria, respectively.

as many as defendant[s] suggest[.]" *U.S. v. Lumiere*, No. 16 CR 483, 2016 WL 7188149, at *6 (SDNY 2016). In turn, the government disclosed the material to all codefendants.

The court must "suppress" all "electronic evidence seized" from the moving defendants and "imaged" under the affected warrants. *U.S. v. Metter*, 860 F. Supp. 2d 205, 215-16 (EDNY 2012) (ordering "blanket suppression," court noting "release to the co-defendants of any and all seized electronic data without a predetermination of its privilege, nature or relevance to the charged criminal conduct only compounds the assault on his privacy concerns"). Additionally, "the district court [must] conduct[] an evidentiary hearing to determine whether the government's case was *in any respect* derived from a violation of the attorney-client privilege." *U.S. v. Schwimmer*, 892 F.2d 237, 245 (CA2 1989) (emphasis supplied). That would include inquiring whether the government disclosed privileged material to any codefendant now cooperating with the prosecution. Otherwise "defendant[s] will suffer a great disadvantage should [the government] be privy to" and able to use against them "privileged information concerning legal advice rendered" by "counsel." *Kalra v. HSBC Bank USA, N.A.*, No. 06 CV 5890, 2008 WL 1902223, at *7 (EDNY 2008).

In sum, a misleading evidentiary presentation infected the warrant's issuance, and attorney-client intrusions aggravated the error. As such, all "fruit of the poisonous tree" must "not be used against [the defendants]" given "the primary illegality." *Wong Sun v. U.S.*, 371 U.S. 471, 488 (1963).

POINT IV

THE SIXTH AMENDMENT – IF NOT THE FIFTH – ENTITLES DEFENDANTS TO EARLY *BRADY/GIGLIO* DISCLOSURE

The disclosure obligations imposed by *Brady v. Md.*, 373 U.S. 83 (1963), *Giglio v. U.S.*, 405 U.S. 150 (1972), and subsequent cases stem from the Fifth Amendment's due process guarantee. And in our circuit, the government need only turn over constitutionally required exculpatory and impeachment information in time for defendants to use it effectively at trial – not immediately on demand or any sooner. *In re Coppa*, 267 F.3d 132 (CA2 2001); *cf. U.S. v. Ruiz*, 536 U.S. 622, 632-33 (2002) (due process "does not require the [g]overnment to disclose material impeachment evidence prior to entering a plea agreement").

In the years since *Coppa* and *Ruiz*, however, the Supreme Court has held that the Sixth Amendment right to effective assistance of counsel extends to plea bargaining, *Lafler v. Cooper*, 566 U.S. 156 (2012); *Mo. v. Frye*, 566 U.S. 134 (2012) – the culmination of "90% or more of federal criminal cases." *Ruiz*, 536 U.S. at 632; *see Frye*, 536 U.S. at 144 (plea bargaining "is not some adjunct to the criminal justice system; it *is* the criminal justice system") (citations and internal quotes omitted).

It is self-evident that counsel cannot mount an effective trial defense without timely *Brady/Giglio* disclosure. By the same token, how can *any* defense lawyer plea bargain effectively, in the sense *Lafler* and *Frye* contemplate, without knowing the relative strengths and weaknesses of the prosecution's case that *Brady/Giglio* disclosure

helps bring to light? Again, the question answers itself. And when it comes to "the negotiation of a plea" – "almost always the critical point for a defendant" – *Brady/Giglio* disclosure is useless unless made well before trial. *Id.* at 1407.

Immediate production of all exculpatory and impeachment information in the government's possession, custody or control is therefore imperative[31] – and independently mandated by the *Sixth* Amendment's Assistance of Counsel Clause – to preserve the eventuality of effective plea bargaining. The Court should order it accordingly.[32]

POINT V

BECKISH AND DEMARIA JOIN ALL APPLICABLE MOTIONS FILED BY THEIR CODEFENDANTS

[31] For just one example, codefendant and presumptive cooperator Peter O'Brien's home was searched on June 29, 2017, yielding two laptops, two hard drives and *15* cellphones. The sheer number of devices, among other factors, suggests they may well contain materially exculpatory or impeaching information within this request.

[32] This motion is a timely one given the rash of *Brady* violations plaguing the Southern District. *See* J. Capeci, "Sovereign District of New York 'Retrains' All Its Prosecutors on 55-Year-Old Rule," Gang Land News (May 24, 2018) (Ex. H) (reporting open court statement by Judge Nathan that USAO had been seriously discredited with her and two colleagues due to rampant withholding of exculpatory and impeachment evidence, prompting officewide *Brady* retraining); *id.*, "Three Years Later, Feds Turn over *Brady* Material in Meldish Murder" (May 31. 2018) (Ex. I) (reporting that SDNY prosecutors "withheld evidence favorable to the defense for three years from lawyers for a pair of Luchese gangsters charged back in 2015 with [a] gangland-style killing"). Even if not constitutionally required, immediate disclosure thus represents an appropriate exercise of supervisory power.

CONCLUSION

Defendants are entitled to the relief they seek.

Dated: New York, NY
July 31, 2018

Respectfully submitted,

/S/

Marc Fernich, Esq.
Robert Caliendo, Esq.
Law Office of Marc Fernich
810 Seventh Ave., Ste. 620
New York, NY 10019
(212) 446-2346

Attorneys for James Beckish

Jeffrey Lichtman, Esq.
Jeffrey Einhorn, Esq.
Law Offices of Jeffrey Lichtman
11 E. 44th St., Ste. 501
New York, NY 10022
(212) 581-1001

Attorneys for Joseph Anthony DeMaria